Notice of Allowability	Application No.	Applicant(s)	
	10/046,167	WATANABE ET AL.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *an amendment and terminal disclaimer filed on 07/31/06*.

2. ☒ The allowed claim(s) is/are *8 and 9*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 1/16/02
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Carl I. Brundidge, Reg. No. 29,621 on September 12, 2006.

The application has been amended as follows:

In the claims,

8. (Currently Amended) An encryption apparatus comprising:

a pseudorandom number generating apparatus for generating a pseudorandom number sequence having a length equal to that of plaintext data to be encrypted; and

an operation section for conducting an exclusive OR-ing operation on the generated pseudorandom number sequence and the plaintext data, thereby calculating ciphertext data and outputting the ciphertext data,

wherein said pseudorandom number generating apparatus comprises:

a state storage section,

a buffer,

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation,

a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock, and

a buffer control section for updating an internal state of said buffer by using ~~the~~ an output of ~~said~~ a buffer transformation section,

wherein said state storage section has a capacity of 3 blocks (where one block has n bits), and said buffer has a capacity of a plurality of blocks, and

wherein said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs, and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

9. (Currently Amended) A decryption apparatus comprising:

a pseudorandom number generating apparatus for generating a pseudorandom number sequence having a length equal to that of ciphertext data, by using information for determining a random number sequence used when generating the ciphertext data to be decrypted; and

an operation section for conducting exclusive OR-ing operation on the generated pseudorandom number sequence and the ciphertext data, and thereby calculating plaintext data, and outputting the plaintext data,

wherein said pseudorandom number generating apparatus comprises:

a state storage section,

a buffer,

a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation,

a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock, and

a buffer control section for updating an internal state of said buffer by using ~~the~~ an output of ~~said~~ a buffer transformation section,

wherein said state storage section has a capacity of 3 blocks (where one block has n bits), and said buffer has a capacity of a plurality of blocks, and

wherein said state transformation section comprises:

a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs, and

an output section for outputting one block data included in said result of the transformation as a partial random number sequence.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet Dada

September 12, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100